REMARKS

By this amendment, claims 1-17 are pending, in which claims 1, 4, and 14-17 are currently amended. Entry of the amendment is proper after this amendment, because the subject matter of the amendment is adequately supported and has previously been searched and considered (e.g. in claims 4 and 13).

The final Office Action mailed April 5, 2004 rejected claims 1-17 under 35 U.S.C. § 102 as anticipated by *Matyas et al.* (US 5,200,999). This rejection is respectfully traversed because *Matyas et al.* does not disclose the features of the claims.

For example, independent claim 1, as amended, recites three different digital signatures of three different **contents** with three different *private keys*. Dependent claims 2-12 incorporate this feature pursuant to 35 U.S.C. § 112, ¶ 4. The first digital signature is recited as follows:

> (b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature of **the first public key** based on *a private key from the certificate authority*;

The second digital signature is recited as follows:

> (d) generating a second certificate, the second certificate including the second public key and a second digital signature of **the second public key** based on *the first private key*;

The third digital signature is recited as follows:

> (f) signing **data to be transmitted** with a third digital signature . . . utilizing *the second private key*;

As explained in the Specification, a configuration such as the one recited in claim 1 enables data to be signed and verify "without requiring a tremendous amount of time or computing power, while at the same time providing a high-degree of security and ease of implementation" (Spec. p. 4, lines 5-7). More specifically, the third digital signature utilizing the second private key can be implemented to address the need for high performance, while the

implementation of the second digital signature can be designed to address the security aspect of the problem (see, e.g., Spec., pp. 5-6). In accordance with an embodiment covered by claim 1, the public key corresponding to private key utilizing in the second digital signature is digitally signed "based on a private key from the certificate authority."

This feature is not shown in *Matyas et al.* In particular, *Matyas et al.* (per Abstract) discloses an approach in which two key pairs are generated for use in a data processing system, in which each key pair is permitted to be used with different public key algorithms in accordance with a private control vector. *Matyas et al.* further discloses that the private keys of these two pairs are encrypted under a "first master control express which is a function of the private control vector" (Abstract). *Matyas et al.* also mentions a PR2 master key "used to generate an authentication signature for the public and private keys kept outside the cryptographic facility" (col. 9:47-50). However, *Matyas et al.* fails to describe a system with "a first digital signature of **the first public key** based on *a private key from the certificate authority*" and "a second digital signature of **the second public key** based on *the first private key*" as recited in claim 1. In fact, *Matyas et al.* does not even describe digital signatures "based on a private key from the certificate authority" and PR2 cannot be both the private key from the certificate authority and the first private key, as that would entail that it is kept outside the cryptographic facility contrary to *Matyas et al.* principle of operation.

The passages of *Matyas et al.* cited in the Office Action, namely cols. 12:28-13:9 and 24:43-26:14, do not support the rejection because there is no description there of a digital signature for a public key.

Furthermore, independent claim 13 recites the following features:

> (b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on *a key pair of a certificate authority*;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature *based on the master key pair*;

(g) encrypting the hash value utilizing the *second private key* as the encryption key; and

These features too are not shown in *Matyas et al.* because, as explained above, the PR2 master key is not kept outside the cryptographic facility. Further, claims 13 also recites:

(c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair;

There is no disclosure in *Matyas et al.* that the PR2 master key is shorter than itself.

Accordingly, independent claim 15, which recites "a digital signature of the short public key based on a long private key longer than the short private key," is also patentable over *Matyas et al.*—as are independent claim 14 ("a short disposable key pair that is shorter than the long master key pair") and independent claim 16 ("wherein the short public key is shorter than the long public key").
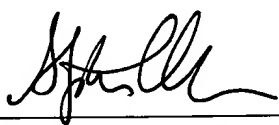
Independent claim 17, as amended, sets forth "verifying the public key based on a digital signature of the public key issued by a certificate authority." For the reasons described above, nothing in *Matyas et al.*, including the PR2 master key, satisfies this feature.

Therefore, the present application, as amended, overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at 703-425-8516 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

_6/7/2004_

Date

Stephen C. Carlson
Attorney/Agent for Applicant(s)
Reg. No. 39929

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. 703-425-8516
Fax. 703-425-8518